

Claims

1. (currently amended) Software ~~from computer-readable medium(s)~~ creating the a user signature ~~portion of a user login account, as at least part of a subject to subsequent validation protocol for login submission,~~ wherein at least part of said signature having at least one user-determined transmission type.
2. (currently amended) Software ~~from computer-readable medium(s)~~ validating a signature comprising a plurality of signals by accessing data from a plurality of keys.
3. (currently amended) Software ~~from computer-readable medium(s)~~ incrementally validating a signature while receiving signature input.
4. (currently amended) A method ~~in software~~ for creating the a user signature ~~portion of a user login account,~~ comprising at least one transmission, ~~as at least part of a said signature subject to subsequent validation protocol for login submission,~~ said method comprising the following steps:
 - a) receiving a user ~~determining~~ determination of a transmission type of at least one transmission;
 - b) recording a plurality of signal types for at least one transmission;
 - e) packaging and recording at least one recorded transmission into at least one key;
 - d) ~~storing at least one key in at least one file.~~
5. (currently amended) A method ~~in software~~ for validating user ~~login submission~~ input data comprising the following steps:
 - a) accumulating possible keys based upon matching key data to initial input data;
 - b) discarding accumulated keys based upon failure to match to subsequent input data until completing validation ~~is completed~~ or by process of elimination impossible.
6. (currently amended) Software according to claim 1 whereby receiving said user ~~determining~~ determination of at least one signal type of at least one transmission of said signature.

7. (currently amended) Software according to claim 6 ~~whereby~~ wherein said user-determined signal type is of a user-determined transmission type.
8. (currently amended) Software according to claim 1, wherein said signature comprising the entirety of a resource access login submission.
9. (currently amended) Software according to claim 2 wherein said validating by accessing data from a plurality of keys stored in one or more files, wherein said keys are in non-contiguous storage locations ~~not-contiguous~~.
10. (original) Software according to claim 9 wherein said keys are stored in the same file.
11. (original) Software according to claim 2 wherein said keys are stored in different files.
12. (currently amended) Software according to claim 2 employing at least one next key trajectory as part of said ~~validating~~ validation.
13. (currently amended) Software according to claim 3, wherein said validating ~~comprising~~ comprises signal matching, whereby said matching may be successful with an inexact match between stored data and corresponding ~~login~~ submitted input data.
14. (original) Software according to claim 3 whereby said validating terminating passively.
15. (currently amended) Software according to claim 14 wherein said terminating passively having been user-determined during ~~creation of~~ creating said signature validation protocol.
16. (currently amended) The method according to claim 4, ~~whereby~~ wherein receiving said user ~~determining~~ determination of at least one signal type of at least one transmission ~~for said subsequent validation~~.

17. (currently amended) The method according to claim 4, ~~whereby~~ wherein receiving said user ~~determining~~ determination of a plurality of transmission types from a plurality of said recorded transmissions.

18. (original) The method according to claim 4 whereby recording a plurality of signal types emanating from a single transmission.

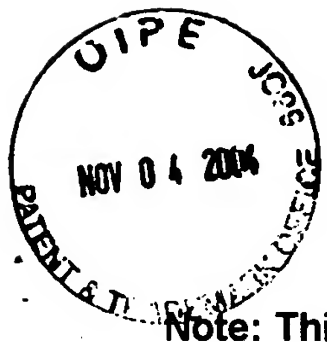
19. (original) Software according to claim 4 storing at least one fake key.

20. (original) The method according to claim 4 wherein packaging at least one next key trajectory in said key.

21. (original) The method according to claim 4 wherein packaging a plurality of next key trajectories in said key.

22. (original) The method according to claim 21 whereby said different next key trajectories are to keys in different files.

23. (original) The method according to claim 4 wherein at least one transmission comprising input from a plurality of devices.



Note: This mailing includes non-fee amendments for two patent applications:

10/067646 Software sentinel

10/090520 Computer login multiplicity